PA 352654

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

4

January 16, 2001

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/174,530***
FILING DATE: ***January 05, 2000***

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

E. Bornett
E. BORNETT
Certifying Officer

01/06.00

PROVISIONAL PATENT APPLICATION TRANSMITTAL

A
PROV

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR 1.53(b)(2).

Docket Number	SANF-24400 (P058)	Type a plus sign (+) inside this box ->	+

INVENTOR(s)/APPLICANT(s)	
FIRST NAME, MIDDLE INITIAL, LAST NAME	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
1. STEVE EPSTEIN	5A Hamarpe Street, Har Hotzvim, Jerusalem 91235, Israel
2. STEPHANIE WALD	5A Hamarpe Street, Har Hotzvim, Jerusalem 91235, Israel
3. YAAKOV BELENKY	5A Hamarpe Street, Har Hotzvim, Jerusalem 91235, Israel
4. ELI HIBSHOOSH	5A Hamarpe Street, Har Hotzvim, Jerusalem 91235, Israel
5. YIGAL SHAPIRO	5A Hamarpe Street, Har Hotzvim, Jerusalem 91235, Israel
6. CHAIM SHEN-ORR	5A Hamarpe Street, Har Hotzvim, Jerusalem 91235, Israel

TITLE OF THE INVENTION (280 characters max)

DIGITAL CONTENT DELIVERY SYSTEM

CORRESPONDENCE ADDRESS

Joel G. Ackerman
Limbach & Limbach L.L.P.
2001 Ferry Building
San Francisco
Phone: 415/433-4150; Fax: 415/433-8716

STATE	CA	ZIP CODE	94111-4262	COUNTRY	U.S.A.

ENCLOSED APPLICATION PARTS *(check all that apply)*

x	Specification *Number of Pages*	9			Small Entity Statement
x	Drawing(s) *Number of Sheets*	2			Other (specify):

METHOD OF PAYMENT *(check one)*

x	A check or money order is enclosed to cover the Provisional filing fees.	PROVISIONAL FILING FEE AMOUNT(S)	$150.00.
X	The Commissioner is hereby authorized to charge any additional filing fees and credit Deposit Account Number: 12-1420		

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government

☐ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE: _____

TYPED or PRINTED NAME: Joel G. Ackerman

Date: January 5, 2000

REGISTRATION NO. *(if appropriate)*: 24,307

CERTIFICATION UNDER 37 CFR §1.10

I hereby certify that this New Provisional Application and the documents referred to as enclosed herein are being deposited with the United States Postal Service on this date January 5, 2000, in an envelope bearing "Express Mail Post Office To Addressee" Mailing Label Number EL151572495US addressed to: Box Provisional Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

SIGNATURE: _____
HOWARD WONG

Date: 01-05-00

Subject: Invention – Digital content delivery system

Inventors – Steve Epstein, Stephanie Wald, Yaakov Belenky, Eli Hilbshoosh, Yigal Shapiro, Chaim Shen-Orr

Date: 5 January 2000

Introduction

The following concept is intended to enable secure distribution and payment assurance for digital content, mainly Audio. This concept can also be applied to other digital content, such as video or data (software, games, etc.).

Background

US Pat. 5,282,249 and 5,481,609 (Cohen et al)

US Pat. 4,748,668 (Shamir et al) and 4,933,970 (Shamir)

Design of the Dallas Semiconductors "Soft Micro" series (50xx)

All references mentioned about and throughout the present specification are hereby incorporated herein by reference.

Concept

The concept involves secure electronic distribution of digital contents (mainly audio), including its being secure from unauthorized playout throughout its lifecycle, and assured payments. The system would support business models based on (possibly concurrent) distribution and payments modes, and rely on a combination of secure hardware and software to prevent / retard hacking.

The security of the system is a result of several basic rules:

- All content are encrypted throughout the system, the only exceptions being at the Headend entry and at the last physical point immediately prior to actual physical use. In the audio example, that point would be the analog voltage signal going to the analog speakers. The physical construction of the integrated circuits handling the content (PM - Playout Module) would be such that no cleartext signal is available outside the IC package.

- The business rules and data are embodied in a "security module" (SM), optionally removable (for example, in a smartcard). If removable, it is referred to as "Renewable Security Module (RSM). RSMs may be "paired" to players, the pairing relationship established either in manufacture or through an on-line connection to the Headend.

- In addition to the SM, business rules rights, credits etc. are maintained at the system Headend. Thus periodic connections to the Headend allow for synchronization and detection of pirate activity. One of the rules may force the user to establish a connection to the Headend on a periodic basis

- Each piece of content includes metadata, which specifically include signed (optionally encrypted) Entitlement Control Messages (ECMs), which specifies entitlements required of the player in order to play out that content.

- Each player would receive – either separately or together with content delivery – Entitlement Management Messages (EMMs), that update the entitlements ("rights") of that player. EMMs may be addressed to groups or individual players.

- The SM / RSM checks requirements embodied in ECMs, and entitlements derived from EMMs, to decide whether the player is entitled to playout the particular content at that time. If the player is entitled, the SM produces the correct Control Word (or Keyword) required to decipher the content.
In addition, PECMs - a special class of ECMs may address specific players, who therefore do not require positive EMMs to enable playout of the specific content. Negative EMMs may prohibit such action, for example by invalidating the player for all playout.

- Most software within the PM and the SM is downloadable. All software that may access any security-associated data can be downloaded only through a secure loader.

The system would support content purchase and playout ether while connected to a central server ("Headend"), or while off-line. Off-line purchases are processed and recorded locally by the SM according to pre-established and changeable business rules. Data regarding off-line transactions is coordinated and cleared between the Headend and each SM upon connection. Specific business rules may prohibit unlimited off-line activity.

Business models

The concept supports two basic distribution models:

- Subscription – only members of "subscribed" groups are entitled for playout of any content earmarked for these groups. Obtaining a subscription depends on payment of a subscription fee – one-time (possibly divided into term payments) or ongoing. The subscription fee may depend on any combination of group and individual subscriber properties – for example, group affiliation or membership in other subscription groups.
Two special cases are "All" group, and "zero subscription fee" case. A combination of these two cases amounts to "free content to all players".
It should be noted that there may be a limit on the current total number of subscription groups per off-line player, since the entitlements and payment items have to be stored within the high-security device, whose memory is at premium.

- Purchase – an individual player may purchase individual pieces or groups of pieces, and with a variety of methods such as outright ownership, rental for a given period of time or number of renderings, etc. The purchase price may be a function of any

parameter within the system, including (but not limited to) group membership, other purchases, and time of purchase and/or download.
Purchase decision may be made either while on-line or off-line. Off-line purchase decisions are handled locally by the SM/RSM, resulting in a limit on the number of such purchases due to the SM's memory limitations.
The use of PECMs overcomes this limitation, allowing an unlimited number of pieces, provided that an two-way on-line connection with the Headend is established at some time following off-line purchase for provision of PECMs.

Both models and all their variations may co-exist within a single system, with parameters under control of the Headend and, to a certain extent, under the player's control.
It should be noted that both distribution models support super-distribution (i.e. content may be delivered to a player by another player, rather than from the Headend, with appropriate payment still going to the right party under Headend control). Super-distribution, copy protection and media transfer (such as recording content on a Flash module in one player and attempting to play it in another player) are subject to business rules that are set by the Headend for particular content, groups, or individual players.
Another form of super-distribution is to support gifts, where the purchaser has paid for the rights and the content is delivered to another user. One method would be to make the purchase from the headend on behalf of the other user: the headend would then send the content and appropriate PECM to the other user.
Also, the model may be simplified – if desired – to handle legacy (i.e. non-encrypted) content. Optionally it may be prevented from handling any legacy content except by going through an encryption process.

The model incorporates several level of encryption, some to take care of minimal requirements from industry organizations (such as SDMI), and some to take care of expected stringent requirements from concerned content providers. Thus, local recording of local content (such as voice memos) may be encrypted to comply with SDMI, but not to the same level as high-value content supplied by the Headend.

The model allows unlimited storage of content, such as in a PC disk, set-top box or any recordable media. Stored content are secure by virtue of their being encrypted, and not playable without going through a PM. For the PM, there is no difference whether the immediate source of the content is the Internet, a broadcast means, or a PC's disk.

Interpretation of business rules and conditions embodied in EMMs, ECMs and PECMs is done in the Security Module (SM). If the SM may be removable / renewable (i.e. RSM - for example, using a smartcard. That module may optionally be easily removable, to enable its service in related or unrelated business applications (such as loyalty cards, purchase of non-digital content items, or any other use). There is an option to exchange data between applications, thus enabling application of credit, loyalty points etc. from one application to another.

Distribution modes

Distribution conduits would be either bi-directional (Internet, Kiosk) or unidirectional (broadcast, IP multicast). Superdistribution .(i.e. content transfer between players) is a sub-case of a unidirectional conduit.

Distribution modes:

- Free – no encryption involved
- Encrypted to all valid players
- Encrypted to subscribers (according to their subscription level), i.e. for a group
- Encrypted for an individual

The scheme is implemented using two-tier encryption: the content to be delivered are first encrypted by a "strong" algorithm A (for example, 3DES), and the "A" key (or Control Word) is encrypted using one of several algorithms, according to the intended purpose of the particular piece.

Optionally, the content is encrypted in several parts, each one having a different encryption mode. This serves the purpose of enabling "free preview" for particular (or all) audiences. Some preview material (such as descriptive text) may not be encrypted at all.

The key/keys, together with the metadata describing the content and its intended uses, are delivered in encrypted and signed packet(s) together with the content. The whole message (content, keys and metadata) is signed (optionally using message digest or other special methods for efficiency of processing) to prevent message changing.

Rights delivery, management and payments

Each player's "rights" or "entitlements" (i.e. which content he is entitled to use under what conditions and for what payment) is delivered in packets which may be delivered either separately or together with a given content package. Entitlement messages are encrypted / signed to either to an individual player or to a group of such players.

The management of entitlements (addition, removal, invalidation, status polling) is done on a separate, secure "renewable" means of storage and computation, such as a smartcard. Thus the entitlements may be delivered via several paths, including ones that do not involve the player at all (such as is done strictly or via a separate conduit. either separate payments

System Security implementation.

Fig. 1 describes the end-to-end software security mechanism in supplying both individual purchased content and subscription content from a headend to an end user device

(player). The overall scheme is similar to that used in Satellite TV Conditional Access (CA) as described in the Cohen & Hashkes patents, except for the facility provided by Personal ECMs (PECMs) to overcome the hardware limitations of secure devices such as the SM.

The headend transmits three types of streams to each end user device:

1. EMMs
2. Content (including metadata and embedded ECMs)
3. PECMs

EMMs, which are securely signed at creation time by the security server, may be delivered over the air in broadcast mode or across the return path in unicast mode to individual or sets of end users. The EMM authorizes each end user to receive Free and subscription content or to purchase Paid content. This is accomplished by sending the SM / RSM within each player a CA Service ID that identifies the rights to a particular content item.

For Free content, an EMM containing a common CA service ID is distributed to all valid players. For subscription content, a EMM containing a specific CA Service ID is delivered to the devices of all end users that subscribed to a particular service (for example - Rock, Jazz, Beatles etc.).

For Paid content, a EMM containing a particular CA Service ID is sent to all end users authorized to purchase this item.

The content production system consists of a content management device that receives files and passes them to either the broadcast station for broadcast to the end user population or to the Web site for on demand retrieval by the end user population. Note that the actual delivery mode is unimportant to this discussion, and local storage outside the player (such as a PC hard disk) or superdistribution would act in exactly the same way. In either or any mode, an end user may retrieve one of three types of content:

1. Free content destined for all valid end users
2. Subscription content destined for only those end users subscribed to this content
3. Paid content destined for only those end users that purchase this content uniquely

Note (encrypted) content may be freely copied from one player (or intermediate storage) to another, but the system poses certain limitations on its decryption and playout:

- Free content may be decrypted by all valid players
- Subscription content may be decrypted by all other end users subscribed to that content service
- Paid content may be decrypted by properly authorized players only following a purchase action for that content. Purchasing may be either on-line (i.e. recorded directly in the Headend) or off-line (i.e. recorded by the SM and cleared through the Headend at a later date)

In order to meet these requirements, the content management station encrypts off-line all content files with a control word provided by the ECM Generator (ECMG) and embeds within he content the actual ECM that is secretly signed by the security server. The control word is derivable from the ECM using a method such as encryption or one-way function as determined by the security server. Note that the security server contains security with a replaceable algorithm synchronized with the replaceable security module in the player.

For free content, there is one or more embedded ECMs that contain the single CA Service that all valid end users are authorized to render. For Subscription content, there is one or more embedded ECM that contains the CA service that only that group may be authorized to render. For paid content, there may be separate types of ECMs embedded in the content. One type of embedded ECM may be associated with the duration of the free preview and contain the CA service of all valid end users. Another type of embedded ECM signifies that this content is purchasable and contains both the unique ID for that Paid content and a CA service of the group that are allowed to purchase this paid content. It will also include all the information necessary to determine the price and business model(s) which applies to that purchase: for instance, rental duration and associated pricing, number of renderings and associated pricing and/or price for outright ownership.

As mentioned, the content is delivered reliably to the end user device via either a uni-directional or asymmetric broadcast mechanism or bisymmetric unicast mechanism and stored in the persistent storage of that end user device (hard disk, Flash chip et al).

Upon playout of the free or subscription content the (optionally renewable) security module, within the player compares the CA Service ID of each ECM associated with the content with those sent via EMM to denote this end user's entitled rights. If there is a match, the security module within the end user device will secretly repeatedly recreate all control words to enable secure decryption of the content and, in the case of music, rendering to the analogue output.

For playout of the paid content, the same mechanism is used to render the preview portion. However, upon reaching the paid ECM, the end user will be required to purchase this content via some user friendly interface (a purchase button for instance). If authorized, upon purchase, the security module will securely mark this purchase by marking a purchase slot containing the unique ID of the content concatenated with a unique ID of the device. Upon playout of this content after purchase, the security module compares the unique content ID contained in the content's ECM and the unique ID of the device with the contents of the slots stored in the replaceable security unit. If there is a match, the file is decrypted and rendered at the analogue output.

Because, the amount of persistent memory (purchase slots) in the security module is finite and we desire to allow each end user to make an infinite number of purchases, we provide a third stream called a PECM or personal ECM. The PECM is a packet that securely authorizes the association between this particular MP3 music item and end user. All PECMs associated with the same content item will generate the same control word;

however, the security module of only the specific player will be able to generate the control word from its PECM. PECMs are also signed securely by the security server.

Whenever the end user connects to the headend[1], the end user device will replace the ECMs, that are tied to persistent purchase slots in the replaceable security module, with PECMS that are just as secure but act autonomously. Hence, this connection will in effect reset the number of content items that the end user may purchase and bring it back to the maximum number supported by the hardware.

Upon playout of content with an associated PECM, the player will first render the preview, as mentioned previously. Upon attaining a PECM, the replaceable secure module will ensure the presence of the appropriate content item and end user device and, if accurate, produce the control word to enable decryption of the paid content and rendering to the analogue output.

Please note that the PECM mechanism was not required for prior art in the TV Conditional Access domain, since secure digital recording of the TV broadcast was not considered. The number of purchase slots required within the SM was therefore rather small, and could be easily implemented with existing technology. For paid and securely-recorded content as considered here, the number of separate pieces purchased and kept could be very large. The PECM mechanism solves this problem, since PECMs do not require any slots.

Also note that the original ECMs are still attached to the encrypted content even while it is playable by PECM. This is very important for the case that the purchased content (together with attached ECMs and PECMs) are copied to another player. The second player would not be able to use the attached PECM, since it is keyed to the first player. The sequence that will occur is that the player would recognize the PECM as such, send it to the SM, and receive an "invalid PECM" response. This will result in the player / SM going to the embedded ECM and acting as indicated – i.e. a purchase will occur, either vis-à-vis the Headend or with the second player's SM. In effect, this results in superdistribution – i.e. the end-users themselves distribute the content, with the system center (Headend) just collecting the payment and reconciling accounts.

Player security

The player is a potential weak link in the system, since it is accessible to potential hackers who would try to analyze it and / or extract the unencrypted content. It would therefore be built around a "secure chipset", which may include one or two chips. The single-chip model is shown in Figure 2.

[1] There are two possible frameworks to ensure headend connection. In the unicast domain (web site), the end user may be forced to connect at least once a day (to fetch EMMs and PECMs), or the device – in the audio case - will only render one or two default songs. In the broadcast domain, the end user may see a purchase meter (similar to the battery meter on laptop computers), which denote the number of purchases remaining. At low remaining purchases, the end user on his own accord will reconnect to reset the purchase meter to the maximum (equivalent to the number of purchase slots).

The main consideration in the chip design (other achieving the desired level of performance) is to avoid having any unencrypted content outside of the secure chip. Thus, external content memory is encrypted (or scrambled), unencrypted data busses do not extend off-chip, and digital-to-analog conversion (D/A) is performed on-chip.

Since the content decoding algorithms (as well as the decryption algorithms) may change over time, at least a part of program memory has to be downloadable. Any program that can access any of the security-related software or data must not be amenable to a change by non-authorized operators. Such program must therefore be loaded only through a secure loader, requiring knowledge of secret passwords and procedures, and optionally Zero Knowledge Test – type authentication, such as Fiat-Shamir.

External program memory and its bus have to be encrypted to deter pirates from reading the program. Since the encryption scheme / keyword for the content memory are more amenable to analysis than that of the more-critical program memory, the two schemes (or at least their keywords) must be different.

In addition, it is desirable to have each individual player device use its own keywords, so that bus readout on two different devices would yield different results. This may be achieved either by each device's random keywords be generated by final test machinery during production, and burned-in into on-chip persistent memory. Another option involves having a true random number generator on-board, generating random keywords. On-chip keyword generation is especially attractive if battery-backup volatile external memory is used, similar to the scheme used by Dallas Semiconductor for their "Soft Micro" line of secure microcontrollers.

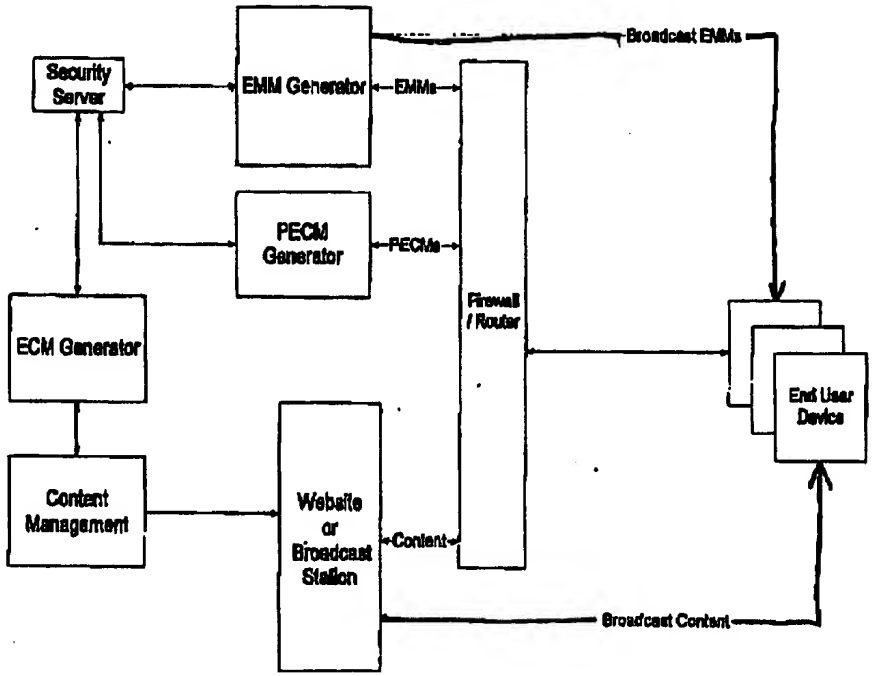
In any event, keywords and other "secret" information must be stored on-chip, to avoid their being exposed to line sniffing. Furthermore, proprietary techniques are used to protect these secrets against invasive attacks using micro-probing equipment. Other proprietary techniques may be used against other attacks, such as Power Analysis, Differential Power Analysis, and Skip / Glitch attacks.

Other essential elements within the secure chipset are:

- Mode set logic and hardware – to enable the same basic chipset to serve the varying requirements of system vendors. A typical implementation would contain one-time memory elements (OTP) or fuses, to force a particular chip into certain modes – for example, use of a high-security RSM vs. no RSM.
- Security algorithms hardware – required to accelerate certain computations such as DES or modulo arithmetic
- Secure clock – several implementations are possible, with all based on non-volatile internal memory. Clock security would be required to prevent hackers from resetting the clock to an earlier (or future) date to obtain some time – dependent rights. One example would be if a desirable music piece was pre-released to be playable only after a certain date, or to bypass rental expiration.

NOTE: Fig 2 shows only security-related elements. Other items such as digital input / output, power supply, reset etc. are not shown.

Fig. 1



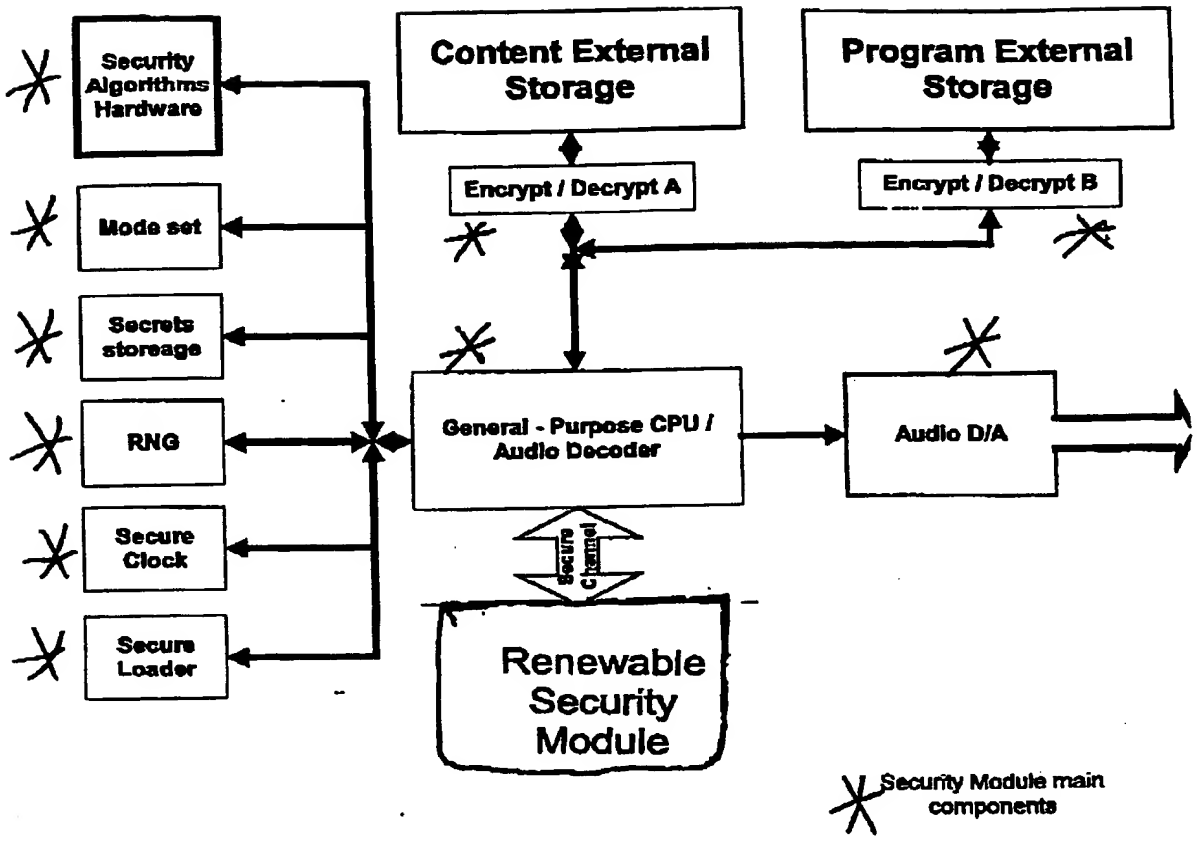

Security Algorithms Hardware
Mode set
Secrets storeage
RNG
Secure Clock
Secure Loader
Content External Storage
Program External Storage
Encrypt / Decrypt A
Encrypt / Decrypt B
General - Purpose CPU / Audio Decoder
Audio D/A
Secure Channel
Renewable Security Module
Security Module main components

Fig. 2